North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Oslo city leaders expecting another round of flooding. City leaders in Oslo, Minnesota, will look into declaring a state of emergency in February because of expected flooding. This comes after the National Weather Service's latest predictions showed a better than 50-50 chance of major flooding in many northern Red River Valley communities. Oslo's mayor said the town will most likely become an island again this year. In the past few years, all the roads leading into town have been closed because of flooding. In Drayton, people are thankful for a new bridge that will stay open longer during flooding than the last bridge because it is built higher. People in town said they would like to have some type of flood protection so they do not have to worry about the river flooding. Crews said they are ready to build up a dike in Drayton again this year. Source: http://www.wday.com/event/article/id/42906/group/Weather/

Tesoro has fire in gasoline unit at Mandan refinery. Tesoro Corp. is assessing the damage from a fire in a gasoline-making unit at its Mandan, North Dakota, oil refinery, a company spokesman said. The blaze, which started January 19 was put out at about 3:30 p.m., he said. The spokesman said all workers were accounted for, and that the refinery is running at a reduced rate. The fire occurred on the north side of the property at an oil furnace, the Morton County emergency manager said. Flow to the oil furnace was stopped. The refinery processes primarily sweet domestic crude oil from North Dakota, the company spokesman said. The 58,000-barrel-per-day plant, built in 1954, manufactures gasoline, diesel fuel, jet fuel, heavy fuel oils, and LPG, he said. Refined products are trucked and shipped by train from Mandan and shipped via pipeline to supply the Jamestown, North Dakota, area, as well as eastern North Dakota and Minnesota. Source: http://www.businessweek.com/news/2011-01-19/tesoro-has-fire-in-gasoline-unit-at-mandan-refinery.html

Regional

(Minnesota) **School building evacuated for the second time this school year.** Officials evacuated a Caledonia, Minnesota, school for the second time this school year January 20 after finding a written bomb threat. A note found at the combined public high school and middle school building said a bomb would go off at 12:40 p.m., the superintendent said. A similar note was found at the school in October. Caledonia district administrators were meeting at 10 a.m. at district offices, which are in the elementary school, when the high school principal got a call about the threat. The principal went to the building, while bus services were called. The high school-middle school was evacuated, and students were brought to the elementary school in about 15 minutes. Police and first responders arrived at the school, and a bomb-sniffing dog searched the building. No explosives were found, and students returned to the school by 1 p.m. Source: http://www.winonadailynews.com/news/article_22a916c2-2518-11e0-99d5-001cc4c002e0.html

(Minnesota) **Man caught with 2 guns at Rochester mall.** A 23-year-old Rochester man is in jail after police say he was caught with two handguns in a duffel bag at Apache Mall in Rochester, Minnesota.

Police say one of the guns was loaded. The man told police he was looking to take the guns elsewhere for target practice. A police captain tells the Post-Bulletin it did not appear the man had any criminal intent. But he said the man has a previous conviction that prohibits him from carrying a firearm. The man met a friend who works at the mall Sunday and told him he had two handguns, briefly showing one to the friend, who notified mall security. Security officers detained the man without incident and took the bag away from him before police arrived. The man has not been formally charged. Source: http://www.startribune.com/local/113969464.html?elr=KArks7PYDiaK7DUqEiaDUiD3aPc:_Yyc:aU7DYaGEP7vDEh7P:DiUs

(Montana) **More snow increases avalanche danger in Cooke City-area mountains.** With another 6 to 8 inches of snow overnight and continued strong wind gusts, the avalanche warning for the mountains around Cooke City, Montana, was bumped to high January 18 on wind-loaded slopes. According to a spokesman with the Gallatin National Forest Avalanche Center, ridge-top winds averaged 25-30 mph with gusts exceeding 40 mph. More snow is expected by January 19. The mountains around Cooke City collected almost 3 feet of new snow in the 72 hours ending mid-day January 18. "With even more snow and strong west to northwest winds, I'm betting that there are many natural avalanches on wind-loaded slopes today which have a high avalanche danger," the spokesman wrote in the morning report. "All other slopes have a considerable danger." Source: http://billingsgazette.com/news/state-and-regional/montana/article_305ff38d-1dfc-58ef-8f41-b4556cf49047.html

(South Dakota) **Teen pleads guilty in SD school threat case.** The South Dakota attorney general said a high school senior who plotted an attack on Sisseton High School in northeast South Dakota pleaded guilty to the sale, transport, or possession of a destructive device. The attorney general said January 20 the 18-year-old suspect of Claire City faces up to 10 years in prison on each count at his February 17 sentencing. The suspect had been charged with a third count of unauthorized possession of a substance with intent to make a destructive device. He was arrested last August after someone told a police school resource officer the suspect had talked about an attack at Sisseton High School. Court files said he wrote about wanting to "become the world's most infamous sociopath." Source: http://www.necn.com/01/20/11/Teen-pleads-guilty-in-SD-school-threat-c/landing_nation.html?&blockID=3&apID=d432a163e89d441dbc02bbde66851c8d

(South Dakota; Nebraska) **Bird deaths linked to poison.** Local officials said January 18 that a poison that poses no risk to humans or pets is believed to be the cause of a large bird die-off in Yankton, South Dakota. More than 300 dead starlings have been found in downtown Yankton since January 17. At a media conference January 18, a Yankton Animal Control officer said DRC-1339, a bird poison used by the U.S. Department of Agriculture (USDA), was the probable source of the deaths. She said a USDA official contacted her January 18 after seeing news of the dead birds. In an interview with the Press & Dakotan, a wildlife biologist confirmed that he was involved with dispersing DRC-1339 at a cattle feedlot in Nebraska about 10 miles south of Yankton. He is with the USDA's Animal and Plant Health Inspections Service Wildlife Services and is based in Lincoln, Nebraska. He said starlings at the livestock facility were targeted for eradication when the poison was put out January 13. Besides starlings, DRC-1339 — which can only be sold to government agencies and qualified pest control officers — is also effective on birds such as crows and blackbirds. It does not affect birds of prey who may eat the poisoned animals. Source: http://www.yankton.net/articles/2011/01/19/community/doc4d36568a9e0bf182406588.txt

National

Radioactive capsules recovered in India. Indian authorities have recovered four radioactive isotope cylinders and detained one person allegedly linked to the apparent theft of the material, the Statesman reported January 15. The capsules turned up inside a public restroom at a low-income neighborhood near the Durgapur Steel Plant, the site of their disappearance. The removal of the capsules prompted concerns among managers, police, and experts about the facility's security measures. The site is continuously overseen by 1,500 personnel with India's Central Industrial Security Force. The capsules are "deadly harmful for human beings and are supposed to be preserved in a secure environment," plant officials said. Experts have expressed concern radioactive material could be dispersed by a radiological "dirty bomb." Source: http://www.globalsecuritynewswire.org/gsn/nw_20110119_7551.php

Berms and boom were largely ineffective responses to oil spill, panel reports. In the National Oil Spill Commission's 400-page report on the largest oil spill in U.S. history, there is analysis that suggests the berms and boom did little to prevent oil from making its way to the Gulf of Mexico coast. However, on January 12, a top adviser to the governor of Louisiana said the effort to create offshore berms to keep oil from coming ashore was backed across the board by public officials in Louisiana, and ultimately by the Army Corps of Engineers and the Coast Guard, which gave the green light. He said, as of now, there is no way of knowing how much oil the berms kept from coming ashore. However, according to the commission report: "Responders knew that in deploying boom they were often responding to the politics of the spill rather than the spill itself." And on the berms, the report noted that BP, which agreed to pay for the project, "estimate[d] the cost to be $360 million, double the entire amount it had spent as of early June in helping the region respond to the oil spill." Source: http://www.nola.com/news/gulf-oil-spill/index.ssf/2011/01/berms_and_boom_were_largely_in.html

International

Nigerian militants threaten attacks on oil sector. A Nigerian militant group January 18 threatened attacks on fuel depots, telling residents and workers to move away and saying it would also hit vehicles transporting petroleum products. The Movement for the Emancipation of the Niger Delta (MEND) warned in a statement e-mailed to news organizations of a "ferocious attack" in response to "the handling of the arrest and detention of our respected brothers". The group was behind years of attacks on Africa's biggest oil and gas industry but many of its commanders accepted an amnesty in 2009, and it was unclear what operational capacity it had left. Not all previous threats have been carried out. "Advance warning for immediate evacuation is hereby issued to residents in close proximity to depots storing petroleum products such as aviation fuel, diesel, kerosene, petrol, propane gas and engine oil," the MEND statement said. MEND was for years the main militant group in the Niger Delta, blowing up pipelines and other installations in what it said was a struggle for a greater local share of the natural wealth. The group's suspected mastermind is held in South Africa for his alleged involvement in the October 1, 2010 bombings. Source: http://www.trust.org/alertnet/news/update-1-nigerian-militants-threaten-attacks-on-oil-sector

More VBIEDs detonated south of the border. As the largely narco-fueled violence in Mexico escalates, the country's crime cartels have resorted to using one of jihadist terrorists' most lethal weapons — the car bomb. Mexico's Secretariat of Public Security (SSP) announced that a "vehicle-borne improvised explosive device" (VBIED) exploded January 19 in front of a muni-police station in Linares, Nuevo Leon, Mexico. The car was a white Jetta from Nuevo Leon and had been parked in the reserved parking space of a high ranking police department official. The SSP further confirmed a second car bomb was detonated in front of a police station in San Nicolas hours later. The VBIED detonated in San Nicolas was in a car that reportedly was abandoned by a man dressed in black just minutes before it exploded. According to eyewitness accounts, three women had jumped out of the vehicle that blew up in Linares only minutes after they allegedly left the scene. Although there were no reported injuries, there was extensive property damage, including to two nearby vehicles that belonged to a local police official. Source: http://www.hstoday.us/briefings/daily-news-briefings/single-article/more-vbieds-detonated-south-of-the-border/c9dc67a90ce542fbd748ac9126b4a89c.html

Olympic Games to be policed at 'severe' threat level. The London Olympics is to be policed at "severe" threat level, the senior officer coordinating security has said. The Assistant Commissioner said the threat of international terrorism was expected to remain at severe when the games starts next year. Up to 12,000 officers will be on duty to ensure the safety of athletes, spectators and guests. Events will be held in 34 venues across England with more than 14,000 athletes from 205 nations taking part. Speaking at the new National Olympic Coordination Centre at New Scotland Yard, he said plans for the Olympics were being revised daily. Senior officers are preparing for terrorists who may target crowded venues and VIPs, as well as organized crooks and petty criminals. The security operations will be coordinated from refurbished offices on the 12th floor of New Scotland Yard. Officials from the police, government, Olympic authorities, and emergency services will work around the clock during the 64-day event. A total of Â£600m has been set aside to pay for security, but ministers have said they hope this could be cut by Â£125m. Source: http://www.bbc.co.uk/news/uk-england-london-12187056

Jihadi cleric Anwar al-Awlaki to jihadists living in the West: Obtain money by any means possible, especially from the U.S. government and its citizens. In a new fatwa issued in the lead article of the fourth issue of Inspire magazine, which was published January 16, a Yemeni-American jihadi cleric encourages jihadists living in the West to assist the financing of jihadi activities through any means possible, including theft, embezzlement, and seizure of property. The U.S. government, and U.S. citizens are singled out as prime targets for these acts. Following are the main points and excerpts from the article: In an attempt to deal with the cash-shortage jihadist groups are facing, the cleric gives religious justification to any actions used by jihadists to obtain money. In the article, titled "The Ruling on Dispossessing the Disbelievers' Wealth in Dar Al-Harb," the cleric deals with the issue by ruling that Western countries are considered dar al-harb [the territory of war], countries on which the rules of war apply. Since this is the case, the cleric says Muslims living in the West are not bound by any laws or contracts that prohibit them to harm their countries of residence: "It is the consensus of our scholars that the property of the disbelievers in dar al-harb is halal [permissible] for the Muslims and is a legitimate target for the mujahidin." Source: http://www.memritv.org/report/en/4921.htm

Ex-banker gives WikiLeaks data on 2,000 private Swiss bank accounts. A Swiss banker handed over two discs of data to WikiLeaks, which could contain evidence of tax evasion and criminal activity

committed by prominent people, BBC reports said. The banker will go on trial for breaking bank secrecy laws. In a statement, the bank told the BBC: "Evidently disgruntled and frustrated about unfulfilled career aspirations, the banker exhibited behavior that was detrimental and unacceptable for the bank, which led to termination of the employment relationship." Authorities in the United States are reportedly urging government agencies to set up programs to identify disgruntled employees who might leak sensitive information. The move comes after whistle-blowing Web site WikiLeaks published thousands of leaked diplomatic cables. Twitter was recently issued with a subpoena by the government to release the personal details of people connected to WikiLeaks. The bank account data is expected to appear on WikiLeaks. Source: http://www.infosecurity-us.com/view/15245/exbanker-gives-wikileaks-data-on-2000-private-swiss-bank-accounts/

Banking and Finance Industry

Brazilian phishing scam targets MasterCareward program. Security researchers warn of a new phishing attack that targets Brazilian credit card owners by spoofing e-mails from MasterCard's Surpreenda (surprise) program. The new campaign was spotted by spam analysts from Commtouch, who notes that unlike classic phishing schemes where users are threateinto exposing their sensitive information, this attack tries to lure them with rewards. order to achieve this they spoof communications related to MasterCard Surpreenda, advantage program that lets credit card owners earn reward points when making purchases. These points can then be spent in "pay one, take two" promotions, where second product can be sent as a gift to someone. The rogue e-mails purport to come from surpreenda@redecard(dot)com.br and bear a title of "Participate in the MasterCard Surprise Promotion - RedeCard" [translated]. It is likely the phishers hijacked a legit e-mail advertising the program and only changed the destination of tlink inside. Source: http://news.softpedia.com/news/Brazilian-Phishing-Scam-Targets-MasterCaSurprise-Program-179345.shtml

Zeus malware now targets online payment providers. The Zeus malware continues to evolve, diversifying away from its target bank sites and their customers, and over to sites with user credentials that allow assets that have a financial value. Money Bookers is an online payment provider allowing users to make online payments without submitting personal information each time. Twenty-six different Zeus configurations targeting Money Bookers have been found. This number does not fall short of some of the highly targeted banks and brands in the world. Another target is Web Money. This is another online payment solution that claims to have more than 12 million active users. Web Money is targeted by 13 different Zeus configurations, with the last one released January 16. As with all the other online payment providers, Zeus steals log-in information and other sensitive information of Web Money users. Source: http://www.net-security.org/malware_news.php?id=1600

Online banking trojan developing fast. Trojan construction kit Carberp, which first emerged in the autumn, appears to be undergoing rapid development, according to reports from sources that include security services provider Seculert. An F-Secure analyst is already calling it the rising star of the banking trojan world. Where the first versions of Carberp were very simple in their construction, newer versions are equipped with a more impressive list of features. It now runs on all versions of Windows, including Windows 7, where, according to TrustDefender, it is able to do its work without requiring administrator privileges. The latest version encrypts stolen data prior to transfer using a random key, which the client registers with the control server. These functions have been added to

Carberp over a period of just a few months. Source: http://www.h-online.com/security/news/item/Online-banking-trojan-developing-fast-1172452.html

E-mails containing malware sent to businesses concerning their online job postings. Recent FBI analysis revealed cyber criminals engaging in ACH/wire transfer fraud have targeted businesses by responding via e-mail to employment opportunities posted online. Recently, more than $150,000 was stolen from a U.S. business via unauthorized wire transfer as a result of an e-mail the business received that contained malware. The malware was embedded in an e-mail response to a job posting the business placed on an employment Web site and allowed the attacker to obtain the online banking credentials of the person authorized to conduct financial transactions within the company. The malicious actor changed the account settings to allow the sending of wire transfers, one to the Ukraine, and two to domestic accounts. The malware was identified as a Bredolab variant, svrwsc.exe. This malware was connected to the ZeuS/Zbot Trojan, which is commonly used by cyber criminals to defraud U.S. businesses. Source: http://www.ic3.gov/media/2011/110119.aspx

Fraudster's money mules in short supply, says Cisco. A new security report from Cisco Systems estimated the amount of stolen online bank account data far exceeds the number of people fraudsters can get to transfer stolen funds, who are known as "money mules." A mule is someone who either knowingly helps or is tricked into moving money from a victim's bank account through their own account and then onto a third party, usually located in another country. Money is transferred from the victim's account to the mule's account, and the mule is then instructed to quickly withdraw the money and do a wire transfer or an ACH (Automated Clearing House) transfer. The ACH system is used by financial institutions for exchanging details of direct deposits, checks, and cash transfers made by businesses and individuals. Despite increasing awareness of the schemes, often advertised as "work-at-home" jobs with generous salaries, many people still get caught up in the frauds. Cisco said in its 2010 Annual Security Report that the ratio of stolen account credentials — which can be acquired through phishing or hacking — to available mule capacity could be as high as 10,000 to 1. Source: http://www.computerworld.com/s/article/9205625/Fraudster_s_money_mules_in_short_supply_says_Cisco_

(Oklahoma) **FDIC warns of fake e-mails.** The Federal Deposit Insurance Corporation (FDIC) is warning consumers of a fraudulent e-mail that appears to be from the FDIC. The fake e-mail says the agency "in cooperation with the Department of Homeland Security, federal, state and local governments" has withdrawn deposit insurance from the recipient's account "due to account activity that violates the Patriot Act." The e-mail also contains a link that the recipient is directed to use to verify identity and account information. However, the e-mail and link are bogus, the FDIC said. "It was not sent by the FDIC," the agency said in a news release. "It is an attempt to obtain personal information from consumers. Financial institutions and consumers should not access the link provided within the body of the e-mail and should not under any circumstances provide any personal information through this media." The FDIC said it is trying to identify the source of the e-mails, and advised consumers to report any similar attempts by sending information to alert@fdic.gov. Source: http://newsok.com/fdic-warns-of-fake-e-mails/article/3532188

FDIC phishing emails scare users with Patriot Act violations. The Federal Deposit Insurance Corporation (FDIC) warns users about an ongoing phishing campaign which produces fake e-mails

purporting to come from the organization. “The e-mail informs the recipient that ‘in cooperation with the Department of Homeland Security, federal, state and local governmentsâ¦’ the FDIC has withdrawn deposit insurance from the recipient’s account ‘due to account activity that violates the Patriot Act’,” the FDIC explains in its alert. Recipients are asked to verify their account information through a system called “IDVerify,” otherwise risk account termination. The link to the ID verification system provided in the e-mail takes users to a phishing page that asks them for personal and financial information. FDIC also notes that malicious software may be loaded onto the recipient’s computer, but does not specify if this is done transparently, in a drive-by download attack, or requires interaction from the user. At least one obank has reiterated FDIC’s alert and is warning their customers about the phishing scam, which, apparently, is not entirely new. Source: http://news.softpedia.com/news/FDIC-Phishing-Emails-Scare-Users-with-Patriot-Act-Violations-178185.shtml

Chemical and Hazardous Materials Sector

Aux Sable liquid products recalls to inspect propane gas; can pose fire and burn hazards. The U.S. Consumer Product Safety Commission, in cooperation with Aux Sable Liquid Products, announced a voluntary recall of propane gas sold in portable cylinders and delievred to storage tanks January 20. The recall involves odorized propane gas delivered for storage tanks or sold in portable cylinders between February 25, 2010 and September 30, 2010. Some of this propane does not have sufficient levels of the odorant that is added to propane to help alert consumers to a gas leak. Failure to detect leaking gas can present fire, explosion and thermal burn hazards to consumers. The amount of propane being recalled equates to 700 rail cars full. So far, no injuries have been reported. The propane was sold and distributed through propane retailers in the following states: Connecticut, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, North Carolina, Pennsylvania, Rhode Island, Tennessee, Vermont, and Virginia. Customers in the affected states should contact Aux Sable immediately to arrange for a free inspection. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml11/11102.html?tab=recalls

Commercial Facilities

(Massachusetts) **Explosives found in Belchertown storage unit.** Local and state police and the FBI are continuing an investigation of a cache of weapons and explosives discovered January 17 at the Amherst Self-Storage Facility on Route 9 in Massachusetts. The Belchertown Police chief said a couple who had recently purchased the facility at an auction reported the find at approximately 1:30 p.m. “When they opened the place up, there were some items found that were disturbing to them,” he said. Items found in one of the storage units at the facility included gunpowder, fireworks, firearms, and some electrical wiring. Belchertown police contacted the state police firearms unit and the bomb squad, as well as the FBI for assistance. Source: http://www.amherstbulletin.com/story/id/195901/

(Washington) **Bomb found on Spokane parade route was lethal, FBI says.** An abandoned backpack found January 17 along the route of Spokane, Washington’s annual Martin Luther King Day march contained a bomb capable of inflicting “multiple casualties,” the FBI has confirmed. The bureau’s terrorism task force is offering a $20,000 reward for information leading to the arrest and conviction of those responsible for planting the bomb. The FBI special agent in charge of the Spokane office

would not discuss what specifically made the bomb so dangerous but said the investigation has become a top priority. “It definitely was, by all early analysis, a viable device that was very lethal and had the potential to inflict multiple casualties,” he said. “Clearly, the timing and placement of a device — secreted in a backpack — with the Martin Luther King parade is not coincidental. We are doing everything humanly possible to identify the individuals or individual who constructed and placed this device.” Two security sources told The Spokesman-Review they received a briefing suggesting the bomb was designed to detonate by a remote device, such as a keyless entry remote for a vehicle or a garage-door opener. The bomb apparently also had its own shrapnel that could have caused significant injuries to anyone near the blast. The bomb was discovered in a Swiss Army-brand backpack that was placed on a park bench at the northeast corner of North Washington Street and West Main Avenue. Two T-shirts were in the bag. One reads “Stevens County Relay For Life June 25th-26th 2010” and another shirt reads “Treasure Island Spring 2009.” The FBI is working with other federal agencies and virtually all local police agencies with the investigation as part of the Northwest Joint Terrorism Task Force. Source:
http://seattletimes.nwsource.com/html/localnews/2013970542_paradebomb19.html

(Utah) **FEMA surveys southern Utah’s flood damage.** The Federal Emergency Management Agency (FEMA) sent teams to southern Utah to inspect the damage caused by December flooding. Washington and Kane counties are hoping FEMA can pay at least part of a multi-million dollar bill for damage that’s still being repaired. In St. George, the damage is evident along the city’s trails and golf courses near the Virgin and Santa Clara rivers. Fox 13 was there as the teams look a close look at the Southgate Golf Course, which had one of its fairways wiped out. “This is going to be pretty devastating for us here in southern Utah. We’ve got four city golf courses, and two of them are greatly affected,” said St. George City’s economic development director. St. George estimates the flooding did about $10 million in damage. Golf is a multi-million dollar business in St. George. The city has made it a top priority to have the courses repaired, setting a deadline of the first week in February. Both counties hope FEMA and state officials can help pay for some of the repair work, fearing local coffers may be unable to handle it. A decision is likely several weeks away. Source:
http://www.fox13now.com/news/local/kstu-fea-survey-damage-flooding-st-george,0,2890974.story

(Florida) **Deputies search for ex-roommate after explosives discovered in Wesley Chapel apartment.** Authorities are looking for a 19-year-old man for questioning about explosives discovered January 13 at an apartment complex in Wesley Chapel, Florida. He was a resident at the Columns at Cypress Point apartments until his roommates asked him to move out, according to the Pasco County Sheriff’s Office. After he left, the roommates discovered improvised explosive devices, molotov cocktails, and other unknown fluids in jars inside the apartment, the sheriff’s office said. Residents were evacuated from a building at 4448 Crabapple Drive for several hours while a Hillsborough County bomb squad removed the devices. No one was injured. It is unknown what the man planned to do with any of the materials, a Pasco sheriff’s spokesman said. Source:
http://www.tampabay.com/news/publicsafety/deputies-search-for-ex-roommate-after-explosives-discovered-in-wesley/1145466

Communications Sector

WikiLeaky phone scam targets unwary in U.S. A new voicemail phishing scam uses the threat of non-existent fines for visiting WikiLeaks to pry money out of panicked marks. Prospective marks are robo-dialed by an automated system that states their computer and IP address "had been noted as having visited the Wikileaks site, and that there were grave consequences for this, including a $250,000 or $25,000 fine, perhaps imprisonment." Potentially panicked victims are given a number to phone to discuss payment options. The scam, which involves the use of spoofed phone numbers, takes advantages of VoIP systems to minimize the cost of calls to crooks, who are probably using stolen access to corporate PBX systems. Source: http://www.theregister.co.uk/2011/01/20/wikileak_vishing_scam/

Trapster hack may have exposed millions of iPhone, Android passwords. Millions of e-mail addresses and passwords may have been stolen from Trapster, an online service that warns iPhone, Android, and BlackBerry owners of police speed traps, the company announced January 19. California-based Trapster has begun alerting its registered users and has published a short FAQ on the breach. "If you've registered your account with Trapster, then it's best to assume that your e-mail address and password were included among the compromised data," the FAQ stated. Trapster downplayed the threat, saying it was unsure the addresses and passwords were actually harvested. "While we know that we experienced a security incident, it is not clear that the hackers successfully captured any e-mail addresses or passwords, and we have nothing to suggest that this information has been used," Trapster said. Source: http://www.computerworld.com/s/article/9205660/Trapster_hack_may_have_exposed_millions_of_iPhone_Android_passwords

At Black Hat, fake GSM base station trick targets iPhones. While his Black Hat DC Conference demonstration was not flawless, a University of Luxembourg student January 19 showed it is possible to trick iPhone users into joining a fake GSM network. The student showed how to cobble together a laptop using open-source software OpenBTS and other low-cost gear to create a fake GSM transmitter base station to locate iPhones in order to send their owners a message. A number of iPhone users in the room expressed surprise they had gotten a message asking them to join the network. The student, who is researching vulnerabilities in cellular networks, said that with the right equipment, the range for the rogue GSM station he built can be 35 kilometers. The student's attack would allow him to take advantage of iPhones lured into his rogue base station to "enable and disable auto-answer on the iPhone" he said, or with an attack payload to record the audio on the iPhone, store it in RAM and then transmit the data that was sniffed. The student said he does not want to encourage data theft, but he does want to get carriers and vendors to improve security in the wireless networks. He noted technology such as femtocells could be used to replace the OpenBTS software, which would only amplify the types of attacks he is investigating. Source: http://www.computerworld.

Criminal charges filed against AT&T iPad attackers. The U.S. Department of Justice (DOJ) will file criminal charges against the alleged attackers who copied personal information from the AT&T network of approximately 120,000 iPad users, the U.S. Attorney's Office, District of New Jersey announced January 17. A suspect will be charged in U.S. District Court in New Jersey with one count of conspiracy to access a computer without authorization and one count of fraud. Another suspect will be charged with the same counts at the U.S. Western District Court of Arkansas. The second suspect made headlines last June when he discovered that AT&T's Web site was disclosing the e-mail addresses and the unique ICC-ID numbers of multiple iPad owners. Claiming he wanted to help AT&T improve its security, he wrote a computer script to extract the data from AT&T and then went public with the information. AT&T said nobody from the hacking group contacted it about the flaw. The hacker was arrested January 18 at an Arkansas courthouse, where he had been facing drug possession charges. Those charges have now been dropped. Source: http://www.computerworld.com/s/article/9205403/Criminal_charges_filed_against_AT_T_iPad_attackers

Critical Manufacturing

Poulan Pro Generators recalled by Husqvarna Professional Products due to fire hazard. Husqvarna Professional Products Inc., of Charlotte, North, Carolina, announced a recall of about 600 Poulan Pro Generators January 20. The carburetor can fail allowing gasoline to leak, posing a fire hazard to consumers. The firm has received four reports of fuel leakage. No injuries have been reported. The recall involves gas-powered Poulan Pro Generators designed for residential use. Models included in the recall are: PP4300, PP6600, PP6600E, and PP7600E, all serial numbers. The generators were sold by Poulan Pro and Husqvarna authorized dealers nationwide from July 2010 through September 2010. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml11/11717.html

Keyless systems on cars easily hacked, researchers say. The passive keyless entry and start systems supported by many modern cars are susceptible to attacks that allow thieves to relatively easily steal the vehicles, security researchers at Switzerland's ETH Zurich University said. In demonstrations using 10 cars from 8 makers, the researchers showed how they were able to unlock, start and drive away the cars in each case, by outsmarting the smart key system. The break-ins were carried out using commercial, off-the-shelf electronic equipment available for as little as $100, the researchers said in a paper describing their exploits. Although the possibility of such attacks on keyless systems has been discussed previously, it has not been clear before if they would be feasible on modern cars, the researchers said. "In this paper, we demonstrate that these attacks are both feasible and practical," they said. Source: http://www.computerworld.com/s/article/9205478/Keyless_systems_on_cars_easily_hacked_researchers_say

Schneider Electric recalls Xantrex GT Series grid tie solar inverters due to injury hazard. Xantrex Technology, Inc., a subsidiary of Schneider Electric, of Livermore, California, announced a recall of about 25,000 grid tie solar converters January 18. A component of the inverter can degrade, causing out gassing within the wiring compartment of the inverter. When arcing occurs, gasses could build and force the compartment cover to be blown off. If the cover is blown off with sufficient force it can injure the user or person, or cause damage to property in close proximity to the inverter. Schneider Electric has received five reports of wiring compartment covers being blown off. No injuries or

property damage have been reported. The recalled inverter converts solar photovoltaic voltages into utility grid voltages; allowing the owner to feed power into the electrical grid. The recalled units were manufactured between September 2005 and August 2010. These products were sold under the Xantrex, Sunpower, and General Electric brands. The solar distributors and system integrators were sold throughout the United States and in Canada from September 2005 through January 2011. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml11/11099.html

LED lamps recalled by Eco-Story due to fire hazard. Eco-Story, of Portland, Maine, announced the recall of about 42,000 LED lamps January 19. When used without a Class II transformer, the lamp can overheat, posing a fire hazard. The company has received two reports of overheated lamps. No injuries have been reported. The recall involves the LED 12-volt lamps with UL number E316865. The lamps were sold to commercial locations, primarily restaurants, from December 2007 through August, 2010. The lamps were not sold directly to consumers. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml11/11716.html

Defense/ Industry Base Sector

Lockheed redesigns F-35B bulkhead. Lockheed Martin has redesigned the bulkhead on the F-35B Joint Strike Fighter (JSF) where the main landing gear meet the airframe to prevent the type of cracking that was found during ground stress tests on the jet, according to Lockheed, and the U.S. Marine Corps Commandant. He revealed the bulkhead has been "re-engineered" during a speech January 13. He was discussing the future of the short take-off and vertical landing version of the JSF and the testing challenges it has been experiencing, saying he believes Lockheed and the Pentagon can solve the jet's engineering difficulties in the next 2 years. Lockheed officials confirmed the reworked bulkhead design, saying the flaw was only found on one plane used for ground tests and that the cracks, revealed in November 2010, did not contribute to the delays in the F-35B's test schedule. Source: http://www.dodbuzz.com/2011/01/13/lockheed-redesigns-f-35b-bulkhead/

Emergency Services

(District of Columbia) **D.C. wants access to thousands more surveillance cameras.** Washington, D.C.'s homeland security department is pressing for access to more security cameras, including ones owned by private businesses and Metro. The D.C. Homeland Security and Emergency Management Agency submitted a plan to tap into private cameras, such as those found at banks or outside office buildings, as well as those at public housing developments, the Washington Examiner reported. The agency already has access to more than 4,500 cameras owned by D.C. transportation and school systems. If approved, the plan would grant the homeland security department access to thousands of more cameras. Officials at the department's joint all-hazards operations center watch the centralized feed from all of the cameras 24 hours per day. By extending the access to surveillance cameras, D.C. joins a number of other major cities, including New York and Baltimore, that already use cameras to fight crime. In the United Kingdom., CCTV, or closed-circuit television, commonly uses surveillance cameras to monitor public spaces and public transportation in an effort to deter crime. There are reportedly more cameras per person in the U.K. than in any other country in the world. While most district surveillance cameras make recordings of the areas they monitor, those recordings are only kept for about 10 days. Source: http://www.wtop.com/?nid=596&sid=2241997

(New Jersey) **Cellphones give feds insight into criminal activity.** When FBI agents wanted to reconstruct the movements of a rogue New York City cop who staged a $1 million perfume heist in Carlstadt, New Jersey, last February, they turned to cellphone records to trace his steps. Using a computer mapping program and "call detail" logs obtained from Sprint Nextel, agents plotted the locations of 42 cell sites in Bergen and Hudson counties and New York to track the suspect's movements as the armed robbery plot unfolded. He was convicted in December 2010. Cellular tracking of criminals — including those who use prepaid mobile phones that cannot easily be traced because there is no subscriber contract — has become a cottage industry for the FBI. Based on current cellphone and texting patterns, cell site data for a typical adult user will reveal between 20 and 55 location points a day — enough to plot his or her movements hour by hour, a federal magistrate judge in Houston noted in October in denying a bid for cell records. The demand for cell site records has drawn criticism from civil libertarians, prompting some courts to take a new look at the legal ground rules for granting access to such data. The Stored Communications Act of 1986 allows prosecutors to obtain court orders for cell site logs merely by showing that the tracking information is "relevant and material" to an ongoing criminal probe. That is a much lower burden than the probable cause standard required under the Fourth Amendment, which guarantees the right of the people to be secure against unreasonable searches and seizures. Source: http://www.northjersey.com/news/114072489_Feds_dialed_in_to_criminals.html?page=all

Police turn to drones for domestic surveillance. Police agencies around the United States soon could have a new tool in their crime-fighting arsenal: unmanned aerial vehicles. Local governments have been pressing the Federal Aviation Administration (FAA) for wider use of unmanned aircraft (UAV) — a demand driven largely by returning veterans who observed the crafts' effectiveness in war, according to experts at New Mexico State University and Auburn University. Police could use the smaller planes to find lost children, hunt illegal marijuana crops, and ease traffic jams in evacuations of cities before hurricanes or other natural disasters. The FAA is expected this year to propose new rules for smaller unmanned aircraft, a process that will include input from the public, an FAA spokesman said. The agency also is talking with the Justice Department and national law enforcement groups "about possibly trying to streamline the process of applying for certificates of authorization" to operate such planes. Drones have flown in the United States for several years but have been limited to restricted airspace and to portions of the borders with Canada and Mexico. One of the chief obstacles to widespread use of UAVs is their inability to "see and avoid" other aircraft as required by federal regulations, a key to flight safety. No local police departments have been authorized to use unmanned aircraft. Source: http://www.usatoday.com/tech/news/surveillance/2011-01-13-drones_N.htm

(New Jersey) **Camden, N.J., to lose nearly half its cops.** There will be fewer cops patrolling the streets of Camden, New Jersey, come January 18. Struggling to close a $26.5 million budget gap, the city with the second highest crime rate in the nation is laying off 163 police officers. That is nearly 44 percent of the force. And Camden will also lose 60 of its 215 firefighters. Some people with desk jobs will be demoted and reassigned to the streets. The mayor's office said the cuts will not affect public safety. "We're still going to protect our residents," said a spokesman for the mayor. Public safety "will remain our top concern. We'll shift our resources to be more efficient with what we have." But police and firefighter union officials said the layoffs will most certainly have an impact. "It's absolutely physically impossible to cover the same amount of ground in the same amount of time with less people," said the president of the Fraternal Order of Police union in Camden. "Response times will be

slower." Source:
http://money.cnn.com/2011/01/17/news/economy/camden_police_layoffs/index.htm?hpt=T2

ENERGY

GAO: Feds need to strengthen smart grid standards and oversight. Federal agencies need to strengthen cybersecurity guidelines and improve oversight of industry efforts to secure smart grid systems and networks, according to a new report from the Government Accountability Office (GAO). While energy companies are using information technology to make the electricity grid more efficient and reliable, those technologies also are creating security vulnerabilities. Federal standards for identifying and mitigating security risks are inadequate, GAO said in a report released January 9. The watchdog found that while the National Institute of Standards and Technology developed and issued cybersecurity guidelines as a result of the Energy Independence and Security Act of 2007, they do not deal with key issues, including the risk of attacks that involve both cyber and physical means. "Until the missing elements are addressed, there is an increased risk that smart grid implementations will not be secure as otherwise possible," GAO said. GAO also found the Federal Energy Regulatory Commission lacks the ability to enforce standards. Source:
http://www.nextgov.com/nextgov/ng_20110114_5416.php?oref=topnews

(Alaska) **Trans-Alaska pipeline restarted after leak repair.** The Trans-Alaska oil pipeline was restarted January 17 after a roughly 58-hour shutdown to allow repair work to deal with a leak. The Alyeska Pipeline Service Co. shut down the 800-mile pipeline January 15 to install a bypass pipe around the leak at Pump Station 1, where the pipeline starts on the North Slope. The shutdown was expected to last 36 hours. A spokeswoman said crews completed work on a 157-foot bypass line to go around the leak, and began the process for restarting the pipeline January 15. After the leak was discovered January 8, Alyeska shut down the pipe for about 84 hours, and production at the more than two dozen oil fields was reduced 5 percent of normal, or about 30,000 barrels per day. As of January 17, Alyeska had recovered about 13,300 gallons of spilled oil from the building where the leak occurred. No oil has been discovered outside the building, the company said. More than 600 people had been involved in responding to the leak, including 375 workers at Pump Station 1. The North Slope oil fields account for about 11 percent of U.S. domestic production. Source:
http://www.bellinghamherald.com/2011/01/17/1820965/trans-alaska-pipeline-restarted.html

Deloitte: Oil, gas industry faces well-organized cyber security threats. Oil and gas companies face cyber security threats, including well-organized efforts by criminal syndicates and terrorist groups. The cybercrime landscape has evolved into highly specialized criminals having sophisticated tools that can routinely evade many security controls, analysts said. A spokesman from Deloitte said the changing threat environment means companies need to evaluate their security strategies, concentrating on espionage and critical infrastructure vulnerabilities. The spokesman urged senior executives to build an effective cyber security program. Executives should ask themselves if their company has enough skilled employees or contractors to mitigate advanced, persistent cyber security threats, he said. Oil and gas companies are at high risk from Web-based malware encounters and cyber attacks because they possess valuable, proprietary data on reserves and discoveries. High downtime cost and attack frequency rates necessitate strong cyber-security programs, the

spokesman said. Source: http://www.ogj.com/index/blogs/health-safety-environment/blogs/OGJ/health-safety-environment-blog/post987_4431226202297142623.html

Food and Agriculture

(Florida) **Florida's non-citrus crop losses from cold could total $370M.** The Florida Department of Agriculture and Consumer Services has estimated 2.5 million cartons or cases of fruits and vegetables were lost due to extremely cold weather during December — not including processed citrus. Officials said another 4 million cartons of produce are expected to be lost before the end of March. Those losses translate into more than $150 million of lost cash sales so far, according to an agriculture department spokesman. In an e-mail January 20, the spokesman said the total losses between December and March will likely top $150 million in cash sales losses, which will result in total economic losses of $370 million. The total estimated losses include expenses for items like labor and fuel that are needed to grow a crop. Some of the heaviest losses have been reported by those growing bell peppers, cucumbers, eggplant, and sweet corn. The preliminary estimates show nearly 1 million bushels of bell peppers alone were lost to the cold. Source: http://www.ocala.com/article/20110120/ARTICLES/110129993/-1/NEWS?Title=Florida-8217-s-non-citrus-crop-losses-from-cold-could-total-370M&tc=ar

(Illinois) **Website allows Illinois farmers to protect sensitive crops from pesticide applications.** Illinois officials are promoting an interactive Internet tool to help protect the state's sensitive crops from drifting pesticides. Organic and specialty growers may enter the locations of their fields on the "Driftwatch" site and pesticide applicators can use the maps to prevent spread of nearby chemical applications. The bureau chief for environmental programs for the Illinois Department of Agriculture said the project requires "shared responsibility" between growers and applicators. He said farmers must accurately register their fields, and applicators must check the site before spraying pesticides. Purdue University developed "Driftwatch" for use in Indiana. U.S. Environmental Protection Agency funds paid for its introduction in Illinois. Michigan, Minnesota, and Wisconsin are starting the program in 2011. Ohio will begin in 2012. Source: http://www.fox59.com/news/sns-ap-il--illinoisfarming-pesticides,0,3114022.story

(Illinois) **Chicago ground beef recall expanded.** Columbus Meat, a Chicago, Illinois, company, has expanded a food recall to include an additional 580 pounds of ground beef patties that may be contaminated with E. coli 0157:H7. Columbus Meat took the action after state inspectors discovered the same batch of contaminated source material was used to produce patties on more than one day. As a result, patties with lot numbers 361361, 361362 and 361364 that were produced on December 29-31 and January 3 have been added to the recall, which also includes 200 pounds of ground beef made December 27. The labels on each package of suspect patties bear an inspection legend shaped like the state of Illinois that contains the establishment number "775." It is believed the patties were distributed in the Chicago area to food-handling establishments such as restaurants and grocery stores. Source: http://www.foodsafetynews.com/2011/01/chicago-ground-beef-recall-expanded/

(Indiana) **52 counties are disaster areas.** Fifty-two counties in Indiana were recently declared disaster areas from the drought that lasted from August 1 through December 31. The U.S. Department of Agriculture (USDA) issued the declaration as a result of losses to the agricultural industry. "This action will provide help to hundreds of farmers who suffered significant production losses," the U.S.

Agriculture Secretary said in a prepared statement. Farmers in Allen, DeKalb, Huntington, Kosciusko, Noble, Steuben, Wells, and Whitley counties are eligible for natural-disaster relief through low-interest emergency loans from the USDA's Farm Service Agency. Source: http://www.journalgazette.net/article/20110120/LOCAL/301209924/1002/LOCAL

(Hawaii) **Botulism fear prompts recall of black bean sauce.** Hawaii Business Group Inc., Barb's Favorite Recipes, and Ohana Seafoods are recalling Barb's Local Style Black Bean Sauce and Ohana Flavors Black Bean Sauce because of possible health risks due to the potential growth of Clostridium Botulinum (botulism), a bacterium which can cause life-threatening illness or death. The sauce was manufactured by First Commercial Kitchen LLC. The Black Bean Sauce is sold in 12-ounce glass jars and labeled as Barb's Local Style Black Bean Sauce or Ohana Flavors Black Bean Sauce. The UPC numbers on the product are 6-75981-42491-8 and 7-02003-72739-6. The recalled sauce was distributed on Oahu and Molokai. A routine inspection discovered the problem. Source: http://www.foodsafetynews.com/2011/01/botulism-fears-prompt-recall-of-black-bean-sauce/

(New York) **Improperly pasteurized milk recalled in New York.** New York State's acting agriculture commissioner alerted consumers January 20 that certain milk products distributed by FingerLakes Farms LLC, from Plant #36-1131, are being voluntarily recalled due to improper pasteurization. Proper pasteurization heats milk in order to effectively eliminate all pathogenic bacteria, such as Listeria and Salmonella. The recalled milk products are sold under the names Ithaca Milk Company Lowfat Milk, and Ithaca Milk Company Cream on Top Whole Milk. Both of these milk products were packaged in quart, half-gallon, and gallon sizes of plastic containers. All of the products have a container code of SELL BY 013111 and were distributed in the Buffalo, Rochester, Syracuse, and Finger Lakes regions. Routine sampling by New York State Department of Agriculture and Markets Milk Control and Dairy Services inspectors, and subsequent analysis of the product by New York State Food Laboratory personnel, revealed the product was improperly pasteurized. Source: http://www.foodsafetynews.com/2011/01/milk-recalled-in-new-york/

(Wisconsin) **200 dead cows found in Wisconsin.** The Portage County Humane Society is trying to figure out what caused 200 cows in Stockton, Wisconsin to die. According to a Portage County Sheriff's Department news release, deputies were dispatched to the town just after 1 p.m. January 14 after they were notified of numerous dead cows lying in a field in the 8000 block of Fourth Avenue. The owner of the cattle allegedly told deputies he had been working with a local veterinarian and suspected the animals died from either the IBR or BVD virus. According to Cattletoday.info, IBR — infectious bovine rhinotracheitis, or red nose — is an acute, contagious virus that usually occurs in the air passages of a cow's head or its windpipe. Cattle of all ages that have not been vaccinated or have not recovered from the disease are susceptible to IBR, the Web site states. BVD — Bovine Virus Diarrhea — can cause numerous problems, according to the site, such as damage to a cow's digestive and immune systems, pneumonia, abortions, calf deformities, and other symptoms. Samples of the dead animals were sent to Madison for testing. The investigation is being handled by the Portage County Humane Society. According to the Portage County sheriff's department, there is no threat to humans or other animals. Source: http://www.wisconsinrapidstribune.com/article/20110115/WRT0101/101150429/1982/WRT04/200-dead-cows-found-on-town-of-Stockton-farm

(New Jersey) **Spoiled ground beef recall expanded.** One Great Burger of Elizabeth, New Jersey, is expanding its January 10, 2011, ground beef recall to include an undetermined amount of additional ground beef products that may have become spoiled, the U.S. Department of Agriculture's (USDA's) Food Safety and Inspection Service (FSIS) announced January 14. The recalled meat is considered adulterated because the company's food safety plan was inadequate to produce safe product. In a continued investigation of the January 10, 2011 recall, FSIS became aware of additional consumer complaints of discoloration and off-odors in the products. The recall involves 4-pound boxes of "Winn Dixie beef patty 100% Beef" containing 16 frozen patties weighing .25-pounds each. Each box bears establishment number "EST. 34575" within the USDA mark of inspection. The products have "sell by" dates of "01/01/11" through "02/27/11" printed on the bottom of each box, followed by the lot code "204110." The products were produced between April 2010 and May 2010 and distributed to grocery stores in Alabama, Florida, Georgia, Louisiana, and Mississippi. Source: http://www.foodproductdesign.com/news/2011/01/spoiled-ground-beef-recall-expanded.aspx

(Colorado) **Ground beef recall in Colorado.** Colorado Meat Packers, a Denver, Colorado, establishment, is recalling approximately 2,234 pounds of beef trim that was improperly labeled and potentially adulterated, the U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) announced January 15. The product label includes "For Cooking Only," indicating it is intended for further processing to apply a full lethality at a federally inspected establishment. Because the product was sent to a federal establishment that does not conduct lethality operations, the product must be removed from commerce. The following product is subject to recall: 2,234 lbs. Combo Bin of All Beef Trimmings. The bin bears the establishment number "EST. 17086" inside the USDA mark of inspection and can be identified by the case code "9002 N." The ground beef trim was produced December 2, 2010 and sent to a federal establishment in Colorado for further processing without testing. Source: http://www.krdo.com/news/26503890/detail.html

(California) **Life Technologies creates salmonella test in wake of major egg outbreak.** A Carlsbad, California company has introduced a genetic test that could make it easier to detect contaminated eggs. Life Technologies said January 13 that its TaqMan salmonella enteritidis detection kit has been cleared for sale by the U.S. Food and Drug Administration. The test can deliver results in about 27 hours, far quicker than more conventional methods that take up to 10 days, the company said. The faster turnaround could help egg producers detect contaminated eggs before they head to markets, said the president and chief executive of United Egg Producers. Federal rules requiring large-scale egg producers to test for the bacteria went into place in July after the salmonella outbreak began. Source: http://www.signonsandiego.com/news/2011/jan/13/life-tech-creates-salmonella-test-after-major-egg-/

United Fresh examines impact of food safety law. The United Fresh Produce Association has released a new white paper that explores the likely effects of the FDA Food Safety Modernization Act. The white paper examines new requirements and regulations under the new law faced by businesses within the fresh produce supply chain. Included in the report are breakdowns on the ramifications for produce grower-shippers, wholesalers and distributors, fruit and vegetable importers, retailers and food service operators, and food transporters. "The FDA Food Safety Modernization Act will mean significant changes for the fruit and vegetable industry," said the senior vice president of public policy for United Fresh. "This white paper gives a quick but exhaustive rundown of the major changes that produce industry members can expect under the new law; all in plain English." According to United

Fresh, in addition to the segment-specific impacts for these sectors, the white paper looks at the legislation's effect on the industry as a whole, including the aspects of the bill that deal with mandatory recall authority for the U.S. Food and Drug Administration (FDA), traceability, foodborne illness surveillance, food safety education and training, protections against bioterrorism, and laboratory testing. The white paper also includes a quick-reference-style chart showing what new developments can be expected by each sector, as well as a timeline for the implementation of all new regulations under the law. Source: http://www.foodsafetynews.com/2011/01/united-fresh-examines-impact-of-food-safety-law/

(New York) **Listeria alert issued for New York herring.** MS Fish Corp., a Brooklyn, New York company is recalling its "Ossie's Schmaltz Herring" due to Listeria monocytogenes contamination. In a news release, the company said the problem was discovered after routine sampling by the New York State Department of Agriculture and Markets Food Inspectors, and subsequent analysis of the product by laboratory personnel, found the product to be positive for Listeria monocytogenes. Ossie's Schmaltz Herring is packed in a 12 oz. plastic container coded 2/0311. It is a non-imported product that is distributed throughout New York City. Source: http://www.foodsafetynews.com/2011/01/listeria-alert-issued-for-new-york-herring/

(Indiana) **Don't eat the Toxic Waste cherry chews.** In a news release posted January 13 on the U.S. Food and Drug Administration (FDA) Web site, an Indianapolis, Indiana company said it was recalling all flavors of its Toxic Waste brand Nuclear Sludge Chew Bars due to elevated levels of lead in the cherry chews. The release said the candy ("hazardously sour," according to its label) is imported from Pakistan and had been distributed nationwide in retail stores and through mail order. Circle City Marketing and Distributing, which does business as Candy Dynamics, issued the recall for Toxic Waste Nuclear Sludge Cherry Chew Bar (UPC 0 89894 81430 6), Toxic Waste Nuclear Sludge Sour Apple Chew Bar (UPC 0 10684 81410 7), and Toxic Waste Nuclear Sludge Blue Raspberry Chew Bar (UPC 0 89894 81420 7). Each chew bar has a net wt. of 0.7 oz (20 g). The company said a recent test performed by the California Department of Public Health indicated a lot (#8288A) of the cherry flavor candy contained elevated levels of lead (0.24 parts per million; the U.S. FDA tolerance is 0.1 ppm). Out of an abundance of caution, Candy Dynamics said, all lots and all flavors of the product distributed from its inception in 2007 through January 2011, are part of the recall. Source: http://www.foodsafetynews.com/2011/01/dont-eat-the-toxic-waste-cherry-chews/

Government Sector (including Schools and Universities)

(Mississippi) **2 schools evacuated after bomb threats.** Officials are working to find the sources of threatening messages left at two Pine Belt, Mississippi, high schools. Students at Oak Grove and Forrest County Agricultural high schools were evacuated January 14 after bomb threats were received. Searches for explosives at both schools turned up nothing. A voicemail message left at Oak Grove High at about 10:30 p.m. January 13 warned of a bomb in the building, while a student at Forrest County Agricultural High School found a note in the hallway January 14 making similar claims. Oak Grove was evacuated shortly after 8 a.m. following the receipt of the message, and FCAHS emptied its halls around 11:30 a.m. After officials searched the OGHS campus and a bomb-sniffing dog combed the area, students were able to return to the school after lunch. The FCAHS principal said the nearly 600 high school students were evacuated to the football stadium without incident.

She said the Forrest County Sheriff's Office assisted school resource officers in searching the premises. Source: http://www.hattiesburgamerican.com/article/20110115/NEWS01/101150322/1002/rss

(Ohio) **Cleveland City Councilman gets police attention after death threats.** A Cleveland city councilman in Ohio is getting police attention after receiving death threats. "It reached its highest point where there was actually a death threat," the city councilman said about threats on his life. He said Cleveland police will give special attention to his home and ward 8 office. The councilman has been at the center of security and policing debates in Cleveland's downtown Warehouse District and said the threats stem from the controversy. Source: http://www.newsnet5.com/dpp/news/local_news/cleveland_metro/cleveland-city-councilman-gets-police-attention-after-death-threats

(Florida) **Officials investigate threat against State Representative William Snyder.** The Martin County Sheriff's Office in Florida, along with other law enforcement agencies, is investigating a threat against a state representative. The representative and law enforcement would not comment on the details of the investigation, only saying a threat was made against the lawmaker and his family. "Certainly a threat against me is something I contend with easily," he said. "It's just a fact of life. I think 33 years in law enforcement, I'm not as jittery as some people might be, but a threat against my family, you saw my grandson here today, I took that very seriously." The representative is in support of a bill similar to Arizona's immigration law. Source: http://www.wptv.com/dpp/news/officials-investigate-threat-against-state-representative-william-snyder

(Pennsylvania) **Feds: Evidence indicates suspect would-be suicide bomber.** Accused of biting two FBI agents, and now painted by prosecutors as a would-be suicide bomber, a 21-year-old suspect will remain in jail pending trial, a U.S. district judge decided January 13. The detention hearing that led to that decision followed a similar hearing the week of January 3, after which a U.S. district magistrate judge ruled the suspect could be released to a halfway house. Both the U.S. attorney's office and the federal public defender's office appealed, with the former saying he should stay in jail and the latter saying he should return to his father's Mayport, Pennsylvania, home. He has remained jailed pending those appeals. Prosecutors presented evidence, including FBI testimony regarding the placement of weapons in the suspect's bedroom at his father's house, and online communications linked to him through his personal laptop. One detailed how an old Buick could be turned into a car bomb using gasoline and tanks — apparently of propane — that could be ignited with a gunshot. Another talked of "being a suicide martyr on your school," or taking school kids as hostages and demanding the freedom of Muslim prisoners. On January 4, agents searched the house in Mayport, in Armstrong County, with a warrant that is still sealed and that emanated from another federal district. The suspect's bedroom contained 14 firearms, thousands of rounds of ammunition and a fake hand grenade, an FBI special agent said. Three of the firearms, including one found under his pillow, were AK-47-type rifles, he said. Agents also found a helmet and gas mask there, and rifle rounds in the bedroom he used at the Natrona Heights home of his mother, who is divorced from his father. Source: http://www.post-gazette.com/pg/11013/1117738-100.stm

(New York) **Feds: NY man threatened US regulators.** A former New York commodities trader is facing charges he made repeated death threats against federal regulators. The suspect from Long Beach,

New York is accused of threatening 47 employees of the U.S. Commodities Futures Trading Commission (CFTC) and other agencies. Prosecutors said he also posted a $100,000 reward on his Web site seeking personal information about several government officials. A criminal complaint said the threats followed a CFTC civil enforcement lawsuit filed against the man. The complaint alleged the suspect has been the subject of various disciplinary proceedings. The suspect was arrested January 13 and ordered held without bail during an initial court appearance January 14 in federal court in Central Islip, New York. Source: http://www.wcax.com/Global/story.asp?S=13846164

(New York) **Man busted for FBI, Congressman threats.** A 55-year-old Hicksville, New York, man has been arrested and accused by authorities of repeatedly calling a U.S. Representative and threatening local and federal law enforcement officials. Nassau County police said the suspect was arraigned January 15 for aggravated harassment after making about 40 rambling calls to the Representative's Queens office over a few weeks, then making seven more on January 13 and 14 after being warned to stop by police. Authorities say that in one of the recent calls, the suspect made threats against law enforcement. He was arrested January 14 and hospitalized for evaluation at Nassau University Medical Center. His arraignment took place by his hospital bed, and he was ordered held on $100,000 bond. Source: http://www.myfoxny.com/dpp/news/local_news/brooklyn/Man-Busted-For-FBI-Congressman-Threats-20110117-APX

(California) **3 shot at Gardena High School; gunman still at large.** A student dressed in black who allegedly shot three fellow pupils at Gardena High School in Gardena, California January 18, surrendered to police in a dramatic end to a standoff. TV footage showed students running out of a classroom where the alleged gunman was hiding. Police then handcuffed the student and took him away. The shooting occurred about 10:30 a.m. on the campus at 1301 W. 182nd St. The alleged gunman apparently pulled the gun out of his backpack. Officials said the gun went off, with one bullet hitting several students, a source told the Los Angeles Times. One students was hit in the head, another in the neck. Their conditions were unknown. A lieutenant said officers were on the scene investigating what happened. The school was placed on lockdown. Source: http://latimesblogs.latimes.com/lanow/2011/01/3-shot-at-gardena-high-school-gunman-still-at-large.html

(California) **Cal State Northridge student charged after officials find explosives, shotgun in his dormroom.** A California State University, Northridge (CSUN) student who threatened several people at the Los Angeles institution is facing two felony charges after police found a shotgun and explosives materials in his on-campus dorm room, according to officials. The 22-year-old suspect allegedly made threats to students and staff on campus and was taken into custody for mental health evaluation January 11, the chief of CSUN police said. Police arrested the suspect January 12 and he is currently in county jail in lieu of a $150,000 bond, according to inmate records. No injuries were reported. The suspect is no longer enrolled at the university and had no previous reported problems at the school, the chief said. He is charged with possession of ingredients to make a destructive device and bringing a firearm onto a school campus, according to the Los Angeles County District Attorney's Office. The suspect is set to appear in court for arraignment January 14 at San Fernando Superior Court. Source: http://www.contracostatimes.com/california/ci_17088326?nclick_check=1

(Massachusetts; California) **High profile education, government sites hacked.** The Web sites of some of the nation's top universities were discovered to be serving up links to bogus online stores offering

everything from popular software by Microsoft to student visas and Viagra, according to a report from security firm zScaler. Portions of Web sites belonging to Harvard University, the Massachusetts Institute of Technology (MIT), and Stanford University were found to be redirecting visitors to phony online Web "stores," using multiple languages, that claim to sell software and other goods at discounted prices. The hijacked Web sites have relatively high search engine rankings, which are used to promote the phony Web stores in search results, Zscaler said. A subdomain of Harvard University's Webs site that belongs to the Chandra X-Ray Observatory was among the domains identified by zScaler as having been compromised. Also, various pages hosted on the domain of MIT belonging to academics, as well as a page belonging to the High-Low Tech group that "integrates high and low technological materials, processes and cultures." At Stanford University, Web sites operated by the Associated Students of Stanford University was compromised, including a Web portal for information about mental and sexual health. There was no clear pattern discernible among the sites compromised, though at least one of the subdomains was hosting the Wordpress blogging software. Source: http://threatpost.com/en_us/blogs/high-profile-education-government-sites-hacked-011311

(Kentucky) **Explosives location map nets charges for students.** Five middle school students in Louisville, Kentucky, have been disciplined after authorities found a map, showing where explosives could be placed at a school. A Jefferson County Public Schools spokeswoman told WAVE-TV in Louisville the students were involved in a fantasy video game and a search of Stuart Middle School found no explosives. The spokeswoman said there was no indication an attack was imminent, but officials must take every threat to student safety seriously. WAVE reported that four students were charged January 13 with misdemeanor criminal conspiracy to commit terrorist threatening and released to their parents. The fifth student was arrested on a charge of felony terrorist threatening. Besides the criminal charges, the students face suspensions and alternative placement. Source: http://www.kentucky.com/2011/01/14/1598665/explosives-location-map-nets-charges.html

Information Technology and Telecommunications

Fake Facebook password change notification leads to malware. An e-mail purportedly sent by Facebook has been hitting inboxes around the world. An attached .zip file that supposedly contains a new password actually contains a backdoor that downloads a MS Word document and opens it. According to Avira, the document contains a few words in Russian and is written in Cyrillic. While users are preoccupied looking at the document and figuring out what it means, a fake AV solution misappropriating the name of Microsoft's Security Essentials solution is downloaded, installed on the system, and starts showing false warnings about the computer being infected. Source: http://www.net-security.org/malware_news.php?id=1599

Soundminer Trojan horse steals Android phone data. Researchers have developed a low-profile Trojan horse program for Google's Android mobile OS that steals data in a way that is unlikely to be detected by either a user or antivirus software. The malware, called Soundminer, monitors phone calls and records when a person, for example, says their credit card number or enters one on the phone's keypad, according to the study. Using various analysis techniques, Soundminer trims the extraneous recorded information down to the most essential, such as the credit card number itself, and sends just that small bit of information back to the attacker over the network, the researchers said. The study was done by researchers from the City University of Hong Kong and Indiana

University. Source:
http://www.computerworld.com/s/article/9205627/Soundminer_Trojan_horse_steals_Android_phone_data

Hacker steals Frogster user data, threatens to shut down servers. An anonymous attacker claims to have stolen log-in data for 3.5 million Frogster accounts, threatening to release user information and shut down the game's servers unless the publisher meets certain demands. In a now-deleted posting on Frogster's message boards, captured by gaming blog Kotaku, a user with the handle Augustus87 demands the Berlin-based company stop closing forum threads, offer more transparency to customers, secure its game clients and user info, and cease its alleged spying of workers' online activities. Augustus87 said if these demands are not met in 2 weeks, he will release information from a collection of 3.5 million accounts for Runes of Magic, Bounty Bay Online, TERA, and other free-to-play games from Frogster. He claims 500,000 of those accounts have been "hacked and verified" so far. Frogster said the data released so far comprises "outdated log-in data from 2007," before its "comprehensive reset initiative." The company has informed the German State Office of Criminal Investigation about the breach, and has formed a task force to determine how the incident occurred. Source:
http://www.gamasutra.com/view/news/32484/Hacker_Steals_Frogster_User_Data_Threatens_To_Shut_Down_Servers.php

Web security cams are a voyeur's delight: Is your IP cam password protected? Web security cameras can be insecure, a researcher from Ars Technica found. The researcher took a spin around the Web checking out live feeds from cameras focused on a number of commercial locations. He was even able to tap into police cameras monitoring an intersection in Texas. In most instances, these cameras were not meant to be offering live video for public consumption. Within the surveillance community, many are turning from closed-circuit/analog cameras to Internet protocol (IP) cameras. While IP cameras are cheaper to install, they can also be easy to locate and to hack into if they are not properly protected. "Finding IP cameras with Google is surprisingly easy," the researcher noted. "Though the information the search engine provides on the cameras themselves is typically little more than an IP address and a camera name or model number, Google still provides those who know how to ask with extensive lists of IP cameras and Web-enabled surveillance systems throughout the world." Source: http://blogs.forbes.com/kashmirhill/2011/01/13/web-security-cams-are-a-voyeurs-delight-is-your-ip-cam-password-protected/?boxes=Homepagechannels

Vulnerabilities in the Boonana Trojan increase the danger. First spotted almost 3 months ago, the Boonana Trojan stood out because of its capability to infect computers running Windows, and machines running Mac OS X. The Trojan nestled itself in the system, and allowed outside access to all files on it. It also seems it has vulnerabilities that can be exploited by other attackers to collect information about the system or — according to a Symantec researcher — even be used to create a completely functional parallel botnet or takeover of the existing one. The Boonana bots are designed to take part of a P2P network and to communicate with each other via a custom-designed communication protocol. Apart from making the identification of infected hosts on a particular IP range almost trivial, the P2P protocol also contains an information-disclosure vulnerability that can be used to detect which operating system the computer is running. According to Symantec, in December

2010, 84 percent of infected systems were running Windows, and 16 percent were running a version of OS X. Source: http://www.net-security.org/malware_news.php?id=1592

SCADA exploit - the dragon awakes. The recent publication of an exploit for KingView, a software package for visualizing industrial process control systems, appears to be having an effect. Threatpost reports that the Chinese vendor Wellintech and Chinese CERT (CN-CERT) have now reacted. The exploit can be used to remotely gain control of a system. In an e-mail to Threatpost, CN-CERT admits it was caught napping when initially notified of the vulnerability by the developer and US-CERT. It was not until November that a further e-mail from US-CERT alerted it to the presence of the vulnerability and led it to rediscover the earlier e-mails sent in September. In November, CN-CERT informed the vendor Wellintech, which is reported to have released a patch December 15 — without, however, informing CN-CERT of the fact and apparently without updating the version available to download from its Web site. A general bug report has now found its way into CN-CERT's database and the vendor has released a patched library. The man who discovered the KingView vulnerabilities, complains on his blog that neither the vendor nor CN-CERT have provided any details of the vulnerability, thereby leaving customers in the dark over the risks it presents. CN-CERT is now planning to review its procedures to ensure it does not miss such e-mails in future and to ensure better contact with vendors while problems are being resolved. Source: http://www.h-online.com/security/news/item/SCADA-exploit-the-dragon-awakes-1169689.html

Facebook U-turns on phone and address data sharing. Facebook appears to have decided to allow external Web sites to see users' addresses and mobile phone numbers. Security experts said such a system would be ripe for exploitation from rogue app developers. The feature has been put on "temporary hold," the social networking firm said in its developers blog. It said it needed to find a more robust way to make sure users know what information they are handing over. "Over the weekend [January 15 and 16], we got some useful feedback that we could make people more clearly aware of when they are granting access to this data. We agree, and are making changes to help ensure you only share this information when you intend to do so," the firm said. The updates would be launched "in the next few weeks," it added and the feature will be suspended in the meantime. Source: http://www.bbc.co.uk/news/technology-12214628

Third-party apps remains security weak point. Microsoft is still burdened with a bad reputation among users for security, although figures show its products are more secure than most on a person's computer, according to new data from the Danish security vendor Secunia. The number of vulnerabilities in software commonly found on PCs shot up by 71 percent between 2009 and 2010, mostly due to problems in third-party applications rather than in the Windows OS or Microsoft apps, said a research analyst director for Secunia. The company released its annual vulnerability report January 18. For its report, Secunia used data from its Personal Software Inspector application, which analyzes PCs to see if the installed programs have the latest patches. Source: http://www.computerworld.com/s/article/9205399/Third_party_apps_remains_security_weak_point

Ransomware continues to pose a threat. Symantec warns against attackers using ransomware. This type of malware blocks access to computers and then asks users to pay for having that privilege returned. Some ransomware locks the computer's desktop and asks the user to send a text message to to a premium rate number to receive back a code that will restore access to the system. Other

ransomware adds to that a change of the desktop background image, which contains the request for money, instructions on how and where to send it, and an embarrassing pornographic image that makes the user less willing to ask for technical help. There is also ransomware that encrypts user files and holds them ransom. Sometimes the encryption key is stored on the computer and the user can decrypt the files if he knows where to look for it, but other times the files are lost for good because there is no guarantee the criminals will send the key to decrypt them even if the victim sends the money. Some ransomware does not even allow the operating system to boot. Source: http://www.net-security.org/malware_news.php?id=1588

First toolkit resulting from ZeuS-SpyEye merger hits the underground market. Security researchers from McAfee warned the first crimware toolkit to result from the ZeuS-SpyEye merger is now available for purchase on the underground market. Earlier in 2011, the security community was surprised to hear rumors ZeuS and SpyEye, two rival threats in the cybercriminal world, would be joined together under a single developer. This unexpected turn of events was supposedly the result of the ZeuS author's intention to retire from the malware-writing scene after a successful run. The new "SpyEye / ZS Builder" was released January 11, which is a SpyEye version enhanced with some of ZeuS' functionality. New features include brute force password guessing, Jabber notification, VNC module, auto-spreading, auto-update, unique stub generation, and an enhanced screenshot system. The builder is much cheaper than ZeuS used to be. The basic version without VNC (remote desktop) and ability to inject code into Firefox pages costs $300, while the price for the full version is $800. Source: http://news.softpedia.com/news/First-Toolkit-Resulting-from-ZeuS-SpyEye-Merger-Hits-the-Underground-Market-178336.shtml

National Monuments and Icons

(California) **Pot growing operation may have been owned by Mexican mafia.** San Luis Obispo County Sheriff's Deputies in California cleared out a major marijuana growing operation located less than 1 mile from Highway 101. San Luis Obispo County Sheriff's Deputies believe the Mexican mafia was behind the 7,000-plant grow. It was located in the Los Padres National Forest about a quarter mile off the highway, near Santa Margarita. The plants were removed back in August, but deputies spent January 19 cleaning up the mess that operation left behind. A National Guard helicopter helped deputies remove pounds of trash, irrigation tubing, fertilizers and camping equipment from the former grow site. Deputies said the operation's reach extends far beyond local land. Nearly 98 percent of these local operations are run by Mexican National Drug Trafficking Organizations. Deputies still have not found the people who were running this grow, so no arrests have been made. Source: http://920kvec.com/Pot-Growing-Operation-May-Have-Been-Owned-By-Mexic/9025697

(Hawaii) **Snow, ice close Haleakala park.** Snowfall and icy road conditions in Hawaii prompted officials at Haleakala National Park to close January 19. Snow fell overnight and could be seen from all around Maui. Park officials closed the park at the 7,000-foot level early in the morning because of the conditions. They began turning visitors away at the gate when the parking lot filled up and rain started falling. The temperatures did not begin rising in the morning and the rains caused the icy road conditions, park officials said. The park may reopen in the afternoon, they said. Source: http://www.kitv.com/news/26543168/detail.html

(Hawaii) **Medical waste continues to wash up at West Oahu beaches.** Medical waste continued to wash up at West Oahu, Hawaii, beaches January 16, hours before another storm hit Oahu, and 3 days after heavy rainfall sent debris from the city's landfill into the ocean. A city councilwoman said she canvassed the beaches January 16 and found more syringes and part of a medical waste container near the landfill's discharge point and Ewa of Ko Olina. The chairwoman of the safety, economic development and government affairs committee said she was getting a group of volunteers together to help clean up the waste reaching the beaches. "My concern is that the government is not treating this situation like the emergency that it is," she said. "We've got hazardous materials, medical waste floating up on our shores, floating in the water and in some areas there are people out swimming in the water." Federal officials closed White Plains Beach and Nimitz Beach in Kalaeloa January 16 because medical waste was found washing up on shore, a U.S. Navy spokeswoman said. City officials are ensuring the landfill operator is continuing with the clean up and discussing measures to prevent a similar discharge. Waste Management Hawaii said employees had been cleaning up every day since the storm and walked Ko Olina and White Sands the morning of January 16. Source: http://www.staradvertiser.com/news/breaking/113857779.html

Postal and Shipping

(Maryland) **FBI links three fiery packages.** The FBI said initial forensic tests have linked the three fiery packages sent to federal and Maryland government officials. The Special Agent in charge of the Baltimore field office said January 18 that while investigators believed they were linked before, they have determined the letters that smoked and popped when opened were manufactured in the same manner. Because the message inside the first two letters got out, the FBI Special Agent said there were concerns the third letter found a day later might be a copycat. He said fingerprint and fiber analysis is expected soon. The FBI Special Agent said investigators are chasing down more than 100 leads in the case and a separate "red cell" team of investigators is exploring what could have motivated the sender. Source: http://voices.washingtonpost.com/crime-scene/update-on-the-news/fbi-links-three-fiery-packages.html

(New York) **Suspected NYC letter bomb may have been greeting card, authorities say.** Police investigated a possible letter bomb at a bank in New York, New York, January 19, according to a department spokesman. No letter bomb was found at the Israeli owned Bank Hapoalim, which is located on the 11th floor of a skyscraper on Sixth Avenue in Midtown Manhattan. The authorities made the determination that there was not a bomb on the bank's premises after X-raying the suspicious package. The letter had no return address and the name of the bank officer to whom it was addressed was misspelled, raising suspicions among bank employees, authorities said. There were wires and a battery in the 6-by-3-inch envelope, but authorities said the envelope may contain an electronic or musical greeting card. It is not clear whether employees who were evacuated from the building have been able to re-enter it. The area was not evacuated. Source: http://news.blogs.cnn.com/2011/01/19/nyc-police-investigate-possible-letter-bomb-at-israeli-bank/?hpt=T2

(Alabama) **HAZMAT teams testing envelopes delivered to Huntsville attorney's office.** Police have a man in custody after a situation at a local office complex in Huntsville, Alabama. They said the man dropped off several envelopes to his attorney at 600 Boulevard South January 18. The incident happened around 1:30 p.m. Police said the envelopes were labeled "Cure to Anthrax," "Cure to

Smallpox," and "Cure to Staph Infections". The attorney's office immediately notified police, due to the labeling on the envelopes. The hazmat team has the envelopes and is working to determine what actually is in each envelope. Police said it appears one of the envelopes only had only small twigs inside. They said the man will be taken for a mental evaluation. The FBI is also involved. Source: http://www.whnt.com/news/huntsvilleandmadisoncounty/whnt-hazmat-teams-respond-to-sitation-at-huntsville-office-complex-01182011,0,6108330.story

(Washington) **Investigators probe suspicious package at office building.** Issaquah Police Department and federal agents continue to probe a suspicious package delivered to a North Issaquah, Washington office building. Police said emergency crews mobilized at about 2 p.m. January 13 after receiving reports of a package containing a suspicious powder. Eastside Fire and Rescue (EFR) and Issaquah Police Department teams responded to the building in the 1600 block of Northwest Sammamish Road, after workers reported concerns about the contents in a package sent to the business. EFR sent a hazardous materials team to retrieve and remove the package. Officials also locked down the building and cordoned off the area for several hours. Responders said three or four workers reported headaches and sore throats. EFR did not transport any workers for medical treatment and the affected workers recovered not long after emergency crews arrived. Crews ended the lock down and allowed workers inside the building to depart at about 5:15 p.m. Investigators interviewed some workers at the scene. The investigation expanded to include the police department, the FBI and the U.S. Postal Inspection Service, the agency responsible for mail-related crimes. Officials had not yet determined the contents of the package. The incident occurred at the Lake Place Office Center near Costco and Costco headquarters. Source: http://www.issaquahpress.com/2011/01/18/investigators-probe-suspicious-package-at-office-building/

(New Hampshire) **Mystery package prompts evacuation, closes downtown block.** A bundle of mail, reported to police as a suspicious package, prompted authorities to evacuate a downtown block and close down through traffic on a portion of Spring Street in New Bedford, Massachusetts, for about an hour January 15. A woman picked up the package, which was wrapped in a Postal Service envelope, and had no address on it, and was bundled with one red and two "vanilla" elastics, she said. She flipped it over, placed it back in the snowbank and called police. Police evacuated the Spring Street block between the Zeiterion Performing Arts Center and the Nativity Preparatory School. That block includes a law office, Supporting Adults for Inclusive Living, commonly referred to as SAIL, Training Resources of America, and parts of the UMass Dartmouth Star Store campus. Authorities sealed off the road with cruisers on both ends of the block. A fire engine was parked farther up Spring Street. Pleasant Street remained open to through traffic. A policeman wearing a vest and helmet approached the package around 12:25 p.m. and motioned for onlookers to back up. Ultimately, police opened the envelope to find a bundle of mail. The street was reopened and people allowed back in the block's buildings by 12:35 p.m. Source: http://www.southcoasttoday.com/apps/pbcs.dll/article?AID=/20110115/NEWS/101150332

Public Health

Data monitoring can aid in hospital infection prevention. As the use of electronic surveillance systems (ESSs) in hospitals for infection prevention and control programs has become more widespread, a new study found that despite evidence these systems may improve efficiency of data collection and potentially improve patient outcomes, ESSs actually remain relatively uncommon in

infection prevention and control programs. The paper, "Electronic Surveillance Systems in Infection Prevention: Organizational Support, Program Characteristics, and User Satisfaction," by researchers at the Texas Health Science Center, published in the American Journal of Infection Control, found "only 23 percent (44/192) of responding infection prevention and control departments had an ESS." No statistically significant difference was seen in how and where infection preventionists who used an ESS and those who did not spend their time. But as the paper pointed out, "little is known about the characteristics of hospitals that have a ESS, user satisfaction with ESSs, and organizational support for implementation of ESSs." Source: http://www.hstoday.us/briefings/daily-news-briefings/single-article/data-monitoring-can-aid-in-hospital-infection-prevention/c875f22d11816b36c3729c1f4d6137bb.html

Hospitals try to curb emergency room crowding. Ochsner Medical Center is one of a growing number of emergency departments trying new approaches to ease crowding. The efforts have added urgency as some experts predict the problem could worsen in coming years. They worry that as millions of people suddenly gain health coverage in 2014 under the new federal health law, they may have trouble finding primary care doctors and will turn to hospital emergency departments instead. The hospital efforts to address the problem have ranged from high-tech options such as smart phone programs that let patients compare waiting times at local hospitals to something as mundane as staggering nursing shifts to better match patient traffic. "Fast tracks," or clinics for patients with simple complaints, are also common. Some hospitals are looking at shaking up and re-engineering their procedures. Ochsner, for instance, created an emergency department protocol called "qTrack." The sickest patients go back immediately to the emergency department's traditional beds, but others go quickly into separate treatment areas with a nice comfortable recliner or to a procedure room for stitches or a cast. Even as emergency departments work on new initiatives, some experts argue that attention should be focused instead on the hospital as a whole. A Rand Corp. scholar and an emergency care physician said such "workarounds" let hospitals off the hook. "The reality is the rest of the hospital doesn't want to deal with the fact that the overcrowded ER is a sure absolute sign of a poorly managed hospital." Source: http://www.msnbc.msn.com/id/41136840/ns/health-health_care/

1b effort yields no bioterror defenses. The Pentagon is scaling back one of its largest efforts to develop treatments for troops and civilians infected in a germ warfare attack after a $1 billion, five-year program fell short of its primary goal. Researchers were unable to break through the limitations of genetic science, according to government officials and specialists in biological terrorism. The Pentagon's next $1 billion for the Transformational Medical Technologies program will focus on better ways to identify mutant versions of Ebola, Marburg, and other deadly viruses. Those are among the genetically modified agents that officials fear could be used by terrorists or rogue states against urban or military targets. The continued flow of money, even with the shift in strategy, should help states retain jobs and research labs focused on this arena. The new strategy represents a return to the drawing board for an ambitious program conceived after the mailing of anthrax to members of Congress and media organizations. Scientists initially set out to develop new medicines capable of attacking viruses that might be altered by terrorists to make them more deadly. After more than 50 research projects by more than 100 contractors, only two experimental medicines have shown promise. Even those are far from being ready for limited clinical tests. A hurdle in the government's effort is that treatments cannot be tested in human clinical trials because it is unethical to expose people to deadly virus in such a study, requiring animals with similar traits as humans to serve as

surrogates. Source: http://www.boston.com/lifestyle/health/articles/2011/01/17/after_1b_spent_pentagon_shifts_strategy_on_bioterror_threats/?page=full

(California) **Man arrested after threats in emergency room.** A Northern California man is facing charges after police said he brought a gun into a hospital emergency room and threatened to start shooting if he did not get faster attention for treatment he was seeking. Police arrested the man after the incident at Mercy Medical Center in Redding, California, around 4:30 p.m. January 15. A Redding police corporal said officers responding to the hospital found a loaded .22 caliber handgun in the man's car and ammunition in his pants pocket. The 24-year-old Anderson man was booked on suspicion of possessing a concealed, loaded weapon, of being an ex-felon possessing a firearm and ammunition, and of resisting arrest. He was being held in lieu of $25,000 bail at the Shasta County Jail. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2011/01/16/state/n135038S88.DTL

Bioterror fears prompt U.S. to keep its smallpox cache. The United States and Russia will fight international efforts the week of January 17 to set a deadline to destroy the last known stocks of smallpox, saying the deadly virus is needed for research to combat bioterrorism. Members of the World Health Organization (WHO) will meet January 19 to begin debating the future of what is left of what was one of the world's most lethal viruses before it was eradicated more than 30 years ago: samples are kept in tightly guarded freezers at the Centers for Disease Control and Prevention in Atlanta and a Russian government lab near Novosibirsk. The U.S. says it needs to maintain the virus samples to develop new drugs and vaccines to counter a potential bioterror attack or accidental release of smallpox from an unsanctioned stock. "Our position is that we need to have the virus collections maintained for the foreseeable future," said a U.S. official familiar with the matter. Russia also believes the virus should be kept for research and is likely to concur with the U.S. position, said an official in the Russian delegation to the WHO executive board. U.S. officials say they need in particular to finish developing and licensing antiviral medications to treat infected people. None are currently approved. Source: http://online.wsj.com/article/SB10001424052748704029704576088032149613692.html?mod=googlenews_wsj

(Oregon) **Beaverton Medical Center evacuated.** A section of Kaiser Permanente Medical Center in Beaverton, Oregon, was evacuated January 13 because of a mentally unstable man. Beaverton police said the man had a baby with him when he walked into the lobby of the building on Southwest Western Avenue. He gave his name to a hospital worker, then laid down on the floor and eventually took off his clothes, officers said. Beaverton police said a portion of the medical center was evacuated while the man was taken into custody. As of 1:30 p.m., the man was undergoing a mental evaluation. The baby is safe and was not injured, police said. It was not immediately clear whether the baby was the man's child or not. Source: http://www.kptv.com/news/26485406/detail.html

FDA targets acetaminophen amounts delivered in prescription painkillers. Federal health officials announced January 13 they were restricting the strength of Percocet, Vicodin, and other popular prescription painkillers to prevent people from suffering severe liver damage from overdosing on one of the main ingredients. The U.S. Food and Drug Administration (FDA) asked drug companies to limit the amount of acetaminophen in all prescription products that combine the drug with other

medications to no more than 325 milligrams per tablet or capsule. Acetaminophen is included at much higher levels in a variety of prescription products with other ingredients, usually powerful painkillers known as opioids. A few examples are Tylenol with Codeine, oxycodone, also known as Percocet, and hydrocodone, which is sold as Vicodin. "Overdose from prescription combination products containing acetaminophen account for nearly half of all cases of acetaminophen-related liver failure in the United States, many of which result in liver transplant or death," an FDA spokeswoman said. The agency also is requiring manufacturers to update labels of all prescription products that combine acetaminophen with other substances to warn of the potential risk for "severe liver injury." The action does not affect over-the-counter products containing acetaminophen. A spokesman for the Public Citizen Health Research Group criticized the agency for failing to address over-the-counter products. Source: http://www.washingtonpost.com/wp-dyn/content/article/2011/01/13/AR2011011306675.html

TRANSPORTATION

(Colorado) **Dangerous lasers light up cockpits of planes flying over Denver.** The FBI in Denver, Colorado, is investigating two separate cases of lasers being pointed into the cockpit of airplanes at Denver International Airport (DIA). Both incidents happened the weekend of January 14. The Federal Aviation Administration told FOX31 News the first one happened January 14, when an Airbus A320 reported a green laser illuminating its cockpit at 13,000 feet. The second incident happened January 17, when an Embraer E170 inbound to Denver reported the same thing. No damage or injuries were reported. Denver was ranked 10th in the country by the FAA in 2010 for the number of laser incidents at DIA. Source: http://www.kdvr.com/news/kdvr-dia-lasers-20110121,0,315871.story

(Washington) **Two Amtrak Pacific Northwest routes closed after mudslides.** Amtrak's Seattle to Vancouver Cascades line and the Empire Builder route to Chicago's Seattle-Everett leg were closed January 19 due to heavy rains and mudslides in Washington State. According to reports, the passengers who regularly rode the trains traveling on the said tracks were offered bus rides to their destinations instead. The Burlington Northern Santa Fe (BNSF) Railway, which operates the two lines, has issued the restriction which will last until January 21, according to Reuters. A BNSF spokesman told Reuters that heavy rains and thawing of snow caused mudslides along many parts of the 155-mile Cascades line, which is the 35-mile Seattle-Everett part of the Empire Builder route. According to Reuters, BNSF tracks have been hit by two mudslides near Everett and Mukilte. Source: http://seerpress.com/two-amtrak-pacific-northwest-routes-closed-after-mudslides/23025/

(Florida) **Police arrest 'suspicious' man at airport.** A man was arrested and turned over to federal authorities January 18 after police said he was taking photos of "sensitive areas" inside and outside of a terminal at Miami International Airport in Miami, Florida. According to the incident report from Miami-Dade County police, the 32-year-old suspect was seen walking through the airport and taking pictures January 11. A sergeant stopped the suspect in the Dolphin parking garage. Police said the suspect did not give them any information about what he was doing or why. In the incident report, the sergeant described his behavior as "evasive." Police said there was no indication the suspect had a plane ticket. After further investigation, federal immigration authorities said the suspect was in the country illegally and wanted for violating U.S. immigration law. Because Miami International Airport is a public facility, anyone is allowed to take video and pictures inside. An official from the

Transportation Security Administration (TSA) told Local 10 that if photography is stepping over the line into surveillance, TSA agents should alert police. Source: http://www.justnews.com/news/26535234/detail.html

FAA: Laser incidents soar, threaten planes. Federal officials said incidents in which lasers have been pointed at planes nearly doubled in 2010, with Los Angeles and Chicago recording the most incidents. The transportation secretary said January 19 that there were 2,836 incidents reported in 2010 in which lasers were pointed at aircraft, compared with 1,527 in 2009. Many of the incidents involve airliners that were in the midst of takeoffs or landings, critical phases of flight when pilots need to be at their most alert. The lasers can temporarily blind pilots. The Federal Aviation Administration said there were 108 laser incidents at Los Angeles International Airport, more than any other airport. Chicago's O'Hare International Airport was next, with 98, followed by airports in Phoenix's Sky Harbor International Airport and San Jose, California, both with 80. Source: http://seattletimes.nwsource.com/html/nationworld/2013975458_apusfaalasers.html

(Florida) **'Suspicious item' reported on plane in Miami, declared safe.** An American Airlines plane was searched and cleared at Miami International Airport in Miami, Florida, January 17 after a "suspicious item" was identified in its cargo hold, the Transportation Security Administration (TSA) said in a statement. American Airlines Flight 930 from Sao Paulo, Brazil, landed in Miami at 8:46 a.m. "In the process of unloading cargo, a suspicious item was identified," TSA said. "Out of an abundance of caution, local law enforcement and EOD (explosive ordnance disposal) arrived on scene to inspect. The item was cleared and declared safe at 10:37 a.m.," the statement noted. TSA did not disclose details. Earlier, an American Airlines spokesman said no explosive material or devices were found on the plane. He said that empty fuse holders were found and described them as like a fuse but not an explosive device. The flight had 169 passengers and 11 crew members on board. Source: http://www.cnn.com/2011/US/01/17/florida.airport.plane/?hpt=T2

(North Carolina) **TSA investigating second airport security breach.** The Transportation Security Administration (TSA) is investigating a security breach involving a JetBlue Airways ticketing agent at Charlotte-Douglas International Airport in Charlotte, North Carolina. It is the second investigation into a security issue at Charlotte-Douglas in recent months. TSA brought a piece of cargo to the JetBlue ticketing counter as part of a sting operation. TSA said it routinely conducts covert and undercover operations to ensure airline employees are following safety rules and regulations. According to WBZ-TV, which first reported the security breach, an undercover TSA agent handed over $100 and asked a JetBlue employee to place a package onto a flight heading from Charlotte to Boston. The package was reportedly put in a passenger's name without that passenger knowing. A spokesperson for JetBlue acknowledged the incident and told NewsChannel 36 the airline is cooperating with the investigation. The ticketing agent involved in the case is no longer employed by JetBlue, the airline said. Source: http://www.wcnc.com/home/TSA-investigating-second-airport-security-breach-113544109.html

(New York) **Suspicious package leads to evacuation of Westchester Airport terminal.** An unattended package in the passenger terminal at Westchester County Airport in Harrison, New York, January 13 led to the evacuation of the facility. The suspicious package, found in the baggage area, turned out to contain food items. Before that was determined, the Westchester County Police Hazardous Devices Unit was called in and the terminal was briefly evacuated. The incident lasted from 11:35 a.m. to

12:20 p.m. Source: http://www.midhudsonnews.com/News/2011/January/14/WCA_evac-14Jan11.html

Water and Dams

(Washington) **Howard Hanson Dam in good shape; but some flooding upstream from Auburn anticipated.** The U.S. Army Corps of Engineers' Seattle District has sent out flood fight teams to the Yakima, White/Puyallup, Green, Snohomish, Skagit, and Chehalis River basins, and the Corps' Emergency Operations Center and Reservoir Control Center were in 24-hour operation, January 17, as warm heavy rainfall continues in western Washington State. Teams deployed to the White and Green river basins are monitoring conditions in the basin and communicating what they see back to the Seattle District's reservoir control center and emergency operations center. Flows are above or near levels — 6,000 cubic feet per second (cfs) along the White River and 9,000 cfs along the Green River — that trigger the Corps to monitor levees 24 hours a day to make on-the-spot visual assessments of river conditions and levee-system integrity. The Corps does not expect the amount of precipitation in the basins of the Green and White rivers to create operational challenges for its dams. The Corps keeps the reservoirs empty at Mud Mountain Dam along the White River, as well as Howard Hanson Dam along the Green River until storage is required for flood risk management, and both had empty reservoirs January 14. The Corps is storing water behind both dams. Source: http://www.seattlepi.com/sound/433557_sound113851039.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**